From: David Wood (obsidian@panix.com)
88 Prospect Park W.
Apt. 4D
Brooklyn, NY 11215

To: FCC

Re: Proceeding 04-295 - Applying CALEA to the Internet

To Whom it May Concern:

I will forbear the obligatory discussion of wiretapping being reprehensible in a free society; let's speak strictly in terms of what passes judicial review and meets constitutional standards.

Traditional telecom-focused surveillance architectures are not a clean fit with Internet communications, speaking both technically and legislatively - perhaps "architecturally."

On the Internet, there is no requirement, and indeed, it is bad engineering, for two parties to communicate via an arbitrary third party. Instead, in proper, efficient designs, two hosts will generally communicate directly. Most importantly, there is no rule - about this, and about hundreds of other details. Different systems may do what they like.

"Wiretapping for VoIP" is thus an impossibly vague concept; different voice-over-IP technologies will vary widely, and may be just as fundamentally dissimilar from each other as they are from traditional telecommunications infrastructure.

One possibly subtle yet enormous difference is that for every major VoIP "phone company" there are dozens of smaller variations that would be impossible outside of a flexible medium like the Internet. All are innovating with distinct hardware and software solutions, and indeed, entire usage models that challenge the basic assumptions of voice communications. Phone numbers themselves are not a requirement for modern Internet voice communications - they are only a recent addition.

It seems obvious to this software engineer that the only realistic alternatives for law enforcement are:

1) Enforcing obvious rules on gateways between Internet telephony and the traditional phone network, so that whether a call originates or terminates with a VoIP provider, the traditional surveillance infrastructure can continue to operate

2) Expanding existing physical-layer surveillance on the Internet to properly handle any type of communications protocols desired.

Point two should bring to mind the hundreds of potential communication protocols for voice alone - many technically indistinguishable from those used by major VoIP providers - spawned from the freedom of anyone to write software and cost-effectively communicate with others.

It is impossible to consider that every author of software capable of communications could anticipate U.S. federal surveillance requirements in their design. It is legally and morally questionable, and technically infeasible to create such a requirement.

We cannot ham-string the whole promising, unpredictable and innovative field of software development just so that it can be safely surveilled. And I mean that literally - we simply lack the power to do it. Even if we somehow convinced ourselves of this frightening logic, other nations would not, and the best we could hope to accomplish would be to legally persecute, marginalize, and expatriate our software development industry.

The burden can only remain on law enforcement to surveil the use of any particular piece of software, just as they must negotiate anyone's property or home when conducting surveillance there, despite many variations in landscaping and architecture.

Best regards,
David Wood